Airsnort unter Windows

--Inhalt--

1) Was ist Airsnort?

Airsnort ist ein Programm, das ursprünglich für Linux geschrieben wurde und mit dem man Wlan-Traffic mitschneiden kann. Diese mitgeschnittenen Fragmente kann man hinterher benutzen, um beispielsweise einen Angriff auf den WEP-Algorithmus zu starten. Dies jedoch selbstverständlich nur, um die Sicherheit des eigenen Systems zu testen.
Unter Windows kann diese Software zwar auch betrieben werden, jedoch ist es hier etwas schwieriger, da die Software, wie gesagt, eigentlich nur für Linux entwickelt wurde. Da dies jedoch die einzige mir bekannte ordentliche Möglichkeit unter Windows ist, umsonst den Datenverkehr mitzuschneiden, verfasse ich diese Anleitung, damit man auch unter Windows von den Funktionen von Airsnort profitieren kann.

2) Vorbereitungen

Um Airosnort benutzen zu können, muss man zunächst sicherstellen, dass die Wlan-Karte den sog. Monitor-Modus (Modus, indem die Karte nur Daten empfängt, jedoch selbst keine Daten aussendet) unterstützt. Darüber hinaus muss sie kompatibel zu den Treibern von Airopeek sein, da Airosnort nur mit diesen Treibern funktioniert. Mit den meisten gängigen Wlan-Karten (z.B. Orinoco Silver/Gold/Classic) sollte dies jedoch kein Problem darstellen. Um zu überprüfen, ob die eigene Karte von Airopeek unterstützt wird, habe ich folgende Liste mit den Daten von der Airopeek-Website zusammengestellt:

11 multi-band cards:

Supported Cards	Notes
3Com 3CRPAG175 Wireless LAN PC Card	New Atheros driver 3.0.1.12
Cisco Aironet CB21AG 802.11 a/b/g Wireless Adapter	Available from WildPackets. Please email sales@wildpackets.com for a quote. New Atheros driver 3.0.1.12
D-Link AirPro DWL-AB650 Multimode Wireless Cardbus Adapter (A/B)	New Atheros driver 3.0.1.12
D-Link AirXpert DWL-	A2 version is reported to

AG650 Wireless Cardbus Adapter (A/B/G)	work. New Atheros driver 3.0.1.12
Linksys Dual Band Wireless A+B Notebook CardBus Adapter (A/B)	New Atheros driver 3.0.1.12
Linksys Dual Band Wireless A+B Notebook MiniPCI Adapter (A/B)	New Atheros driver 3.0.1.12
Linksys WPC55AG Dual-Band Wireless A+G Notebook Adapter (A/B/G)	Only versions v1.0 and v1.1 are supported. New Atheros driver 3.0.1.12
Netgate 5354 Aries2 MP 802.11a/b/g Wireless Mini PCI Card	New Atheros driver 3.0.1.12
NetGear WAG311 802.11a/g Wireless PCI Adapter	New Atheros driver 3.0.1.12
NetGear WAB501 Dual Band Wireless Adapter (A/B)	New Atheros driver 3.0.1.12
NetGear WAG511 802.11a/b/g Dual Band Wireless PC Card (A/B/G)	Only v1.0 and v2.0 are supported New Atheros driver 3.0.1.12
Proxim Gold ORiNOCO 802.11a/b ComboCard Model 8460	New Atheros driver 3.0.1.12
Proxim Gold ORiNOCO 802.11b/g ComboCard Model 8470-WD	New Atheros driver 3.0.1.12
Proxim Gold ORiNOCO 802.11a/b/g ComboCard Model 8480-WD	New Atheros driver 3.0.1.12
ORiNOCO 8481 Silver 802.11a/b/g ComboCard (A/B/G)	New Atheros driver 3.0.1.12
SMC EZ Connect 2.4Ghz/5Ghz Universal Wireless Cardbus Adapter (2335W) (A/B)	New Atheros driver 3.0.1.12
SMC EZ Connect Universal 2.4GHz/5GHz Wireless Cardbus Adapter SMC2336W-AG (A/B/G)	New Atheros driver 3.0.1.12

802.11a cards:

Supported Cards	Notes
Cisco Systems AIR-CB20A Wireless LAN PC Card	Known Cisco Firmware Issue and Cisco Drivers
D-Link AirPro DWL-A650 Wireless Cardbus Adapter	Atheros AR5000 Driver
D-Link AirPro DWL-A650 rev.B Wireless Cardbus Adapter	New Atheros driver 3.0.1.12
Intel(R) PRO/Wireless 5000 LAN Cardbus Adapter	Atheros AR5000 Driver
Intel(R) PRO/Wireless 5000 LAN 3A Mini PCI Adapter	Atheros AR5000 Driver
LinkSys Instant Wireless PC Card (WPC54A)	Atheros AR5000 Driver
NetGear HA501 Wireless Adapter	Atheros AR5000 Driver
Proxim Harmony 802.11a Network Adapter (Model 8450)	Network services are not restored after quitting AiroPeek on Windows 2000 Atheros AR5000 Driver
Proxim Skyline 802.11a Network Adapter (Model 4030)	Network services are not restored after quitting AiroPeek on Windows 2000 Atheros AR5000 Driver
SMC EZ Connect 802.11a Wireless Cardbus Adapter (2735W)	Atheros AR5000 Driver
Sony 802.11a Wireless LAN Adapter (PCWA-C500)	Atheros AR5000 Driver

See the 802.11 multi-band cards for additional adapters that support 802.11a.

802.11b cards:

Supported Cards	Notes
2Wire Wireless PC Card	Agere Driver
3Com 3CRWE737 AirConnect Wireless LAN PC Card	Symbol SYM24 Driver
Avaya Wireless PC Card	Agere Driver

Agere/Lucent ORiNOCO Wireless LAN PC Card	Silver cards and ORiNOCO Classic Gold card (8410-wd) are supported. Proxim's new ORiNOCO Gold card (8420-wd) is not supported. Agere Driver
Agere/Lucent ORiNOCO Wireless LAN Mini PCI	Agere Driver
Air@Hawk LD-WL11/CB Wireless PC Card	Download Realtek Driver
Air@Hawk LD-WL11/PCI3 Wireless PCI Adapter	Download Realtek Driver
Belkin 11Mbps Wireless Desktop Network Card	F5D6001 version 3 only Download Realtek Driver
Belkin 11Mbps Wireless Notebook Network Card	F5D6020 version 3 only Download Realtek Driver
BenQ AWL200(R) Wireless LAN Mini PCI Card	Download Realtek Driver
Buffalo WLI-CB-B11 Wireless LAN Adapter	Download Realtek Driver
Buffalo WLI-PCM-L11/GP Wireless LAN Adapter	Agere Driver
Buffalo WLI-PCM-L11G Wireless LAN Adapter	Agere Driver
Cisco Systems 340 or 350 Series Wireless LAN PC Card	Known Cisco Firmware Issue and Cisco Drivers
Cisco Systems AIR-MP20B Wireless Mini PCI Card	Known Cisco Firmware Issue and Cisco Drivers
Cisco Systems MPI350 Wireless Mini PCI Card	Known Cisco Firmware Issue and Cisco Drivers
Compaq WL110 PC Card	Agere Driver
Connect2Air WLAN E-1100 PC-Card	Agere Driver
Corega WLCB-11 V2 Digital	Download Realtek Driver
Dell TrueMobile 1150 Series Mini PCI Card	Supported on Windows XP Agere Driver
Dell TrueMobile 1150 Series PC Card	Agere Driver
Digital China Wireless	Realtek Driver

Cardbus Adapter	
D-Link Air DWL-510 Wireless PCI Adapter	Realtek Driver
D-Link Air DWL-520 Wireless PCI Adapter	rev. D only Realtek Driver
D-Link Air DWL-610 Wireless Cardbus Adapter	Realtek Driver
D-Link Air DWL-650 Wireless Cardbus Adapter	rev. M- version 3 only Download Realtek Driver Version P1 is not supported.
D-Link Air DWL-660 Wireless PC Card	Agere Driver
Edimax EW-7106 Series Wireless LAN CardBus Adapter	Realtek Driver
ELSA AirLancer MC-11	Agere Driver
ELSA Vianect WLAN MC-11	Agere Driver
Ericsson DSSS Wireless LAN PC Card	Symbol SYM24 Driver
Fujitsu 802.11b Wireless LAN Adapter (A)	Agere Driver
I-Gate 11M PC Card	Agere Driver
Intel(R) PRO/Wireless 2011 LAN PC Card	The 2011B card does not work with AiroPeek. Please use the 2011 card. Symbol SYM24 Driver
Joynet WLAN PC Card	Agere Driver
LANCOM Systems AirLancer MC-11	Agere Driver
LevelOne WPC-0101 11Mbps Wireless PCMCIA CardBus Adapter	Realtek Driver
Linksys Wireless-B Notebook Adapter	WPC11 version 4 only Realtek Driver
NCR WaveLAN/IEEE PC Card	Agere Driver
NEC Corporation Wireless PC Card	Agere Driver
NETGEAR MA521 802.11b Wireless PC Card	Realtek Driver

Nortel Networks e-mobility 802.11 Wireless LAN PC Card	Symbol SYM24 Driver
Onair PC Card (INT)	Agere Driver
Onair PC Card (EMB)	Agere Driver
PLANET WL-3553 Series Wireless LAN CardBus Adapter	Realtek Driver
PLANET WL-8303 Series Wireless LAN PCI Adapter	Realtek Driver
PLANEX GW-NS11X 11Mbps Wireless LAN Card	note: X only Realtek Driver
RoamAbout 802.11 DS (Enterasys)	Agere Driver
Samsung SEW-2001p Card	Agere Driver
Samsung SEW-2001m Card	Agere Driver
Skyward PC Card	Agere Driver
Sony PCWA-C100 Wireless PC Card	Agere Driver
Sony PCWA-C150 Wireless PC Card	Agere Driver
SPEED TOUCH PC Card	Agere Driver
Symbol Spectrum24 11 Mbps DS Wireless LAN PC Card	Symbol SYM24 Driver
Toshiba Wireless LAN Mini PCI Card	Agere Driver
Toshiba Wireless LAN PC Card	Agere Driver
WARPSTAR WL11C (PC-WL/1C)	Agere Driver
Westell 802.11b PC Card	Agere Driver
Wireless LAN Adapter/AeoHammer C110	Realtek Driver
Xircom Wireless Ethernet Adapter	Known Cisco Firmware Issue and Cisco Drivers

See the 802.11 multi-band cards for additional adapters that support 802.11b.

802.11g cards:

Supported Cards	Notes
D-Link AirPlus Xtreme G DWL-G650 Adapter	Rev. B1 is supported, Rev. A1 is not supported. Rev. C1 is reported to work. Rev. B2 is reported to work in Windows XP. Rev. B5 is not supported. New Atheros driver v3.0.1.12

Wie man unschwer erkennen kann, wird also eine Vielzahl von Karten unterstützt. Um den passenden Treiber nun zu installieren, wählt man ihn aus der Liste aus (auch zu finden unter http://www.wildpackets.com/support/product_support/airopeek/hardware) und lädt ihn in ein beliebiges Verzeichnis herunter. Anschließend öffnet man den Gerätemanager (Start -> Einstellungen -> Systemsteuerung -> System -> Karteikarte “Hardware” -> Gerätemanager) und wählt dort die gewünschte Wlan-Karte aus. Diese klickt man mit einem Rechtsklick an und wählt anschließend den Punkt “Eigenschaften”. Nun öffnet man die Karte “Treiber” und klickt auf “Treiber aktualisieren”. Nun zunächst “Weiter” anklicken und dann den Punkt “Alle bekannten Treiber für das Gerät in einer Liste anzeigen und den entsprechenden Treiber selbst auswählen” anwählen. Nach einem weiteren Klick auf “Weiter” wählt man die Schaltfläche “Datenträger” an und gibt hier das Verzeichnis, in das man den Treiber entpackt hat, an. Nun installiert man diesen Treiber für die Wlan-Karte, auch wenn Windows möglicherweise Warnmeldungen ausgibt.
Um Airsnort benutzen zu können, benötigen wir selbstverständlich noch das eigentliche Programm. Dies kann hier http://www.mirrors.wiretapped.net/security/packet-capture/airsnort/airsnort-0.2.6.tar.gz herunterladen. Nach dem Download wird das Paket entpackt und ein neuer Ordner mit dem Namen Airsnort erstellt (NICHT in dem soeben entstandenen Airsnort-Ordner!). Hier wird das Programm später seinen Platz haben.

3) Airopeek

Jetzt testen wir zunächst, ob der Monitor-Mode funktioniert. Tut er dies nicht, wird auch Airsnort nicht funktionieren. Eine gute Möglichkeit, dies zu testen, ist, sich die Demoversion von Airopeek herunterzuladen. Diese bekommt man hier: http://www.wildpackets.com/products/demos/apwnx.
Nachdem man diese heruntergeladen hat, installiert man Airopeek NX und startet das Programm. Hat man nun die Möglichkeit, in den Monitor-Mode zu wechseln, funktioniert alles und man kann das Programm wieder beenden. Funktioniert es nicht, wurde möglicherweise der Treiber nicht richtig installiert oder die Karte wird nicht unterstützt (Tip: Im Ordner /driver des Airopeek-Verzeichnisses befinden sich ebenfalls die nötigen Treiber für die Wlan-Karten!).
Ich gehe nun jedoch davon aus, dass das Versetzten der Karte in den Monitor-Mode funktioniert. Nun beenden wir Airopeek wieder und fahren mit der Installation der Runtimes fort:

4) Runtimes, etc.

Um Airsnort benutzen zu können, benötigen wir neben den passenden Treibern und dem eigentlichen Airsnort-Programm noch diverse Runtimes. Folgend die Links zu diesen Runtimes:

http://www.gimp.org/~tml/gimp/win32/glib-2.4.5-20040903.zip
http://www.gimp.org/~tml/gimp/win32/gtk+-2.4.9-20040903.zip
http://www.gimp.org/~tml/gimp/win32/pango-1.4.1.zip
http://www.gimp.org/~tml/gimp/win32/atk-1.6.0.zip
http://www.gimp.org/~tml/gimp/win32/libiconv-1.9.1.bin.woe32.zip
http://www.gimp.org/~tml/gimp/win32/gettext-runtime-0.13.1.zip

Der Inhalt der .zip-Dateien wird nun in den eben erstellten Ordner Airsnort entpackt. Dadurch sollten die Ordner “bin”, “etc”, “include”, “lib” und “share” sowie die Dateien “COPYING.LIB-2” sowie “README.libconf” entstehen.
Darüber hinaus muss man aus dem entpackten Airsnort-Archiv noch die Datei Airsnort.exe aus dem Ordner “bin” in den Ordner “bin” des selbst erstellen Airsnort-Ordners kopiert werden sowie die Dateien “peek.dll” und “peek5.sys” aus dem Installationsverzeichnis von Airopeek ebenfalls in den “bin”-Ordner von dem selbst erstellten Airsnort-Ordner. Anschließend sollte Airsnort lauffähig sein.

5) Verzeichnisstrukturen

Die Verzeichnisstruktur sieht wie folgt aus:

airsnort:
bin
etc
include
lib
share
COPYING.LIB-2
Readme.libconf

bin:
airsnort.exe
asprintf.dll
charset.dll
envsubst.exe
gettext.exe
gettext.sh
gspawn-win32-helper.exe
iconv.dll
iconv.exe
intl.dll
libatk-1.0-0.dll
libgdk_pixbuf-2.0-0.dll
libgdk-win32-2.0-0.dll
libglib-2.0-0.dll
libgmodule-2.0-0.dll
libgobject-2.0-0.dll
libgthread-2.0-0.dll
libgtk-win32-2.0-0.dll
libpango-1.0-0.dll

libpangoft2-1.0-0.dll
libpangowin32-1.0-0.dll
ngettext.exe
pango-querymodules.exe
peek.dll
peek5.sys

etc: gtk-2.0
pango

include: autosprintf.h
iconv.h
libcharset.h
libintl.h
localcharset.h

lib: gtk-2.0
locale
pango
asprintf.lib
charset.lib
iconv.lib
intl.lib
libiconv.a
libintl.a

share: doc
locale
man
themes

oder ihr nehmt einfach mein zusammengeschnürtes paket:

airsnort.zip

So, hiermit ist mein HowTo beendet. Ich hoffe, ich konnte euch behilflich sein und viel Spaß beim Scannen!
Hinweis: Ich übernehme keinerlei Haftung für Missbrauch der hier angebotenen Informationen bzw. Software, sowie für Schäden jeglicher Art, die durch die Anwendung der Software oder der Informationen aus diesem HowTo entstehen könnten. Dieses HowTo ist keinesfalls als Hilfe zur Ausführung irgendwelcher illegalen Aktivitäten gedacht und soll auch nicht als solche verstanden werden.

Phate

Copyright 2005 by Phate (phate@tectic.de) and http://www.tectic.de